

Chapter 7

Safety and Security of Space-Enabled Education/Learning and Research

MAREK CZAJKOWSKI

Jagiellonian University

ORCID 0000-0003-4276-4984

Abstract: Educational/learning and research satellites can be put in danger in various ways, by various methods, and with varying effects. (1) The process of wearing out or unintentional damage/destruction of satellites concerns individual craft and happens occasionally. (2) Intentional attacks may have a limited and temporary impact on a satellite's operation or may cause serious structural damage resulting in malfunctioning of the satellite or even its fragmentation. (3) An increasing amount of debris in space is resulting in a growing number of collisions which further pollute orbits. This may lead to the so-called Kessler syndrome, a hypothetical situation in which the growing number of collisions in orbit would eventually lead to the cascade effect, rendering whole regions of near-Earth space contaminated to an extent that would make them unusable.

Keywords: International security, space security, space safety, counterspace measures, ASAT weapons, space debris, Kessler syndrome

Executive Summary

Satellites are frequently used for research and education/learning activities, either as carriers of scientific instruments or for supportive purposes (communication, positioning, timing, etc.). Therefore, the safety and security of the operation of these systems directly and indirectly impact the security of research and education/learning activities. Space systems operations may be jeopardized in many ways due to man-made or natural causes, and the severity of related dangers increases in time. This refers particularly to the

growing threat of contamination of the space environment caused by remnants of defunct satellites and their parts, launch vehicles, and other items left in space. In most cases, this space debris remains in orbit for a very long time, which means the danger of collisions producing more junk increases and will continue growing at a pace relative to the increase in the number of objects launched into space. It is even possible that a massive cascade effect (i.e., Kessler syndrome) will occur in the near future, resulting in the rapid destruction of a large number of satellites and rendering some orbits unusable. To date, efforts intended to mitigate the degradation of the space environment have not had a significant mitigating effect.

Introduction

Since the beginning of the Space Age, particularly within the last decade or two, numerous important education/learning aids and scientific instruments have been placed in outer space. Furthermore, education facilities such as universities and research centers increasingly rely on communication and positioning, navigation, and timing (PNT) services provided by various satellite constellations. This way, satellite-derived services have become important, in some areas even critically important, for numerous efforts undertaken by educators, students, and scientific teams worldwide. Consequently, the safe operation of space systems has been increasingly vital to the overall security of these activities. However, the safety and security of space infrastructure cannot be taken for granted; on the contrary, it may be jeopardized in many ways. This part of the report will depict existing and prospective threats to space education/learning and research space systems. It will focus on providing a comprehensive list and describing such threats with an accompanying assessment of the likeliness of their occurrence. The follow-on article will also present a broader political and technical context referring to threats to space architecture along with instances of their manifestations.

Safety and Security of Space Systems

By definition, a space system is a set of functionally connected elements designed to provide service or services due to the utilization of a device perma-

nently located in outer space;¹ it is also often referred to as a satellite system. It essentially consists of three segments: (1) a satellite (orbiter) in orbit around the Earth or another celestial body, (2) a ground station used for controlling an orbital craft and receiving/exchanging data from it, and (3) a communication link between these two. This definition applies to all satellite systems, including education/learning and research ones. Usually, multiple satellites are connected with one or more ground stations via radio or laser communication devices, forming a complex structure labelled a constellation. Some space systems provide their services directly to end users on the ground, and user segment such as GPS receivers or satellite phones are also present in these cases.

Almost all objects sent to space circle celestial bodies along trajectories called orbits, which are closed paths of circular or elliptical shape. The vast majority of spacecraft belonging to space systems operate in the Earth's orbits; only a small number of scientific instruments are located around other celestial bodies, including the Sun. Just a few space vessels follow open trajectories that will eventually lead them out of the Solar System. The following argument will refer to space systems in the Earth's orbits where most educational/learning and research activities are being performed.

Satellite systems provide their services in a very complex and hostile outer space environment, which impacts the safety of their operations in many ways. Furthermore, there are various actual and potential situations in which individual segments of space systems may become a target of malicious activity by state or non-state actors. Thus, we refer to the safety of space systems as far as unintentional threats to their operations are concerned and to security with regard to intentional ones. Note that the distinction between "safety" and "security" works well in English, but other languages such as German, French, and Russian do not fully reflect this distinction.

Threats to Education/Learning and Research Space Systems

Due to the characteristics of outer space and human activities there, most of the threats in space can impact educational/learning and research systems

¹ Marek Czajkowski, "Space-Based Systems and Counterspace Warfare," in *Routledge Handbook of the Future Warfare*, eds. Artur Gruszczak and Sebastian Kaempf (Routledge, 2024).

the same way as every other satellite system. There are no specific dangers that might refer only to the part of overall space architecture that is the main subject of this argument; however, some may concern it to a lesser extent. Thus, the list of threats to space systems presented below is not subject-specific; nevertheless, it entails not only a general description of various dangers that may hamper space systems operations but also some considerations referring specifically to educational/learning and research systems. The argument below is, to a great extent, based on the following publications: *Global Counterspace Capabilities 2024*,² *Space Threat Assessment 2024*,³ and *The Physics of Space Security*;⁴ other sources will be referred to separately. Threats to space safety and security may be the most generally divided into two already mentioned categories: non-intentional and intentional.

Non-intentional Threats to the Operation of Space Systems

This category of threats entails two subcategories, natural and man-made, and two tiers, primary and secondary.

Primary natural threats stem from the destructive characteristics of the space environment itself. Firstly, every object sent to space is subjected to several types of radiation, which gradually degrade its components, causing damage or even making satellites inoperable and uncontrolled. Occasionally, during so-called solar storms, radiation significantly grows, increasing the possibility of the orbiting craft being damaged. Secondly, low gravity, exposure to vacuum, and solar heat also contribute to the relatively quick degradation of satellite components, which may also cause a loss of control over a craft. Eventually, every satellite ends its operation due to the wearing out of its components caused by the harsh conditions they are subject to in space.

² Brian Weeden and Victoria Samson, *Global Counterspace Capabilities 2024* (Secure World Foundation, 2024). <https://www.swfound.org/publications-and-reports/2024-global-counterspace-capabilities-report>.

³ Clayton Swope et al., *Space Threat Assessment 2024*, (Center for Strategic and International Studies, 2024) https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-04/240417_Swope_Space_Threat_0.pdf?VersionId=DDeJ0EkYnF5W7POfMJHVGjkkxEVeTx3o0.

⁴ David Wright, Laura Grego and Lisbeth Gronlund, *The Physics of Space Security* (American Academy of Arts and Sciences, 2005). <https://aerospace.csis.org/wp-content/uploads/2019/06/physics-space-security.pdf>.

The third primary natural threat to satellite systems stems from the fact that space in the vicinity of the Earth, where most of the human space activity is being conducted, is abundant with micrometeoroids, celestial bodies of a mass less than one gram. Micrometeoroids very frequently impact spacecraft surfaces, contributing to the degradation of the structure of components mentioned above. Additionally, there are less abundant but more dangerous larger bodies called meteoroids, some of which are massive enough to significantly damage or destroy spacecraft on impact. Generally, the smaller the meteoroids are, the more frequently they can be encountered in the Earth's vicinity.

Critically important is that most satellites made inoperable due to natural causes remain in space for a very long time. They slowly change orbit, lose components, and sometimes disintegrate. Consequently, every satellite finally turns into a single piece of space junk or even multiple pieces of debris, which litter the extraterrestrial environment, particularly the most commonly used Low Earth Orbits (LEOs). Consequently, the growing number of uncontrolled satellites and other smaller debris increases the possibility of collisions, which produce even more space junk. Thus, space debris produced due to natural causes form what we can term the secondary threat to space systems, as even the smallest uncontrollably orbiting item, like a tiny splinter of metallic structure, can inflict significant damage on a satellite, particularly on delicate surfaces such as solar panels. Therefore, unintentionally, almost every satellite becomes a threat to others once it goes offline.

The threat of damage or destruction due to collision with space debris applies to every kind of satellite in more or less the same way, relative to the layer of near-Earth space they occupy; the more populated by spacecraft a given layer is, the higher contamination, and consequently, the higher the risk of damage or destruction of orbiting craft (except the lowest usable orbit where atmospheric drag cause deorbiting of debris within weeks or months).

Summarizing to this point, natural conditions in space cause every object permanently stationed in orbit to wear out or be damaged/destroyed due to natural causes in a rather short time. Uncontrolled objects and their fragments, space junk, remain in orbit as a second generation of natural threats:

man-made but created by natural causes. Thus, the risk of damaging and destroying educational/learning and research satellites in the Earth's orbits due to collisions with space junk, particularly in LEO, is not negligible, even if it is not high at the moment. What, however, is particularly important and should be noted at this point in the argument is that the increasing amount of debris, matched with ever-growing space activities, naturally causes a steady increase in the risk of collisions. It may eventually lead to the so-called "Kessler effect," envisioned as early as the late 1970s.⁵ This is a hypothetical situation in which the growing number of collisions in orbit would eventually lead to the cascade effect, quickly rendering whole regions of near-Earth space contaminated to an extent that would make them unusable.

Unintentional threats to the operation of space systems may also directly stem from human activities. The first and the most obvious is placing satellites in orbit, as every craft, even before it goes offline, potentially endangers other orbiters. The more of them inhabit a certain orbital plane or certain altitude, the greater the danger of collisions or other interferences. Some orbits are so "crowded" that satellites are frequently forced to alter their flight paths to avoid dangerously close passages with other craft or space debris. Overall, collisions in space are unavoidable, and every one of them further increases the risk of future accidents of that kind. Therefore, the very nature of space, where objects remain for a very long time, even if defunct or torn to pieces, combined with ever-increasing space activities, brings unavoidable threats to all satellites.

Other unintentional threats to satellite systems are technical glitches and human errors, which may result in satellites going offline or even fragmenting before they naturally wear out; nevertheless, they contribute to the expansion of space debris with all the effects described above.

Intentional Threats to the Operation of Space Systems

This section discusses the means used to deprive satellite owners of the benefits stemming from missions space systems perform. In essence, it refers

⁵ Donald J. Kessler and Burton G. Cour-Palais, "Collision Frequency of Artificial Satellites: The Creation of a Debris Belt," *Journal of Geophysical Research* Vol. 86, no. A6 (1978): 2637–2646. <https://archive.org/details/d14ac03deada9364f8bb1fd236dfdbbacb1d/page/n9/mode/2up>.

to situations in which a satellite system is attacked one way or another, leading to interruption or cessation of operation due to temporal or permanent damage or destruction. In general terms, educational/learning and research satellites can be targeted by malicious actors in the same way as other space systems. However, they are less likely to become targets during military operations conducted by nation-states because they are usually much less important from the point of view of strategic concerns. On the other hand, non-state actors may be interested in disrupting educational/learning and research space systems for criminal or commercial reasons. Furthermore, even if not directly targeted, educational/learning and research space systems may suffer the already described secondary effects caused by the increased number of space debris due to combat operations in space. Thus, it is necessary to enumerate all intentional threats to the operation of satellite systems, as all of them may impact the security of space systems either as primary threats or via secondary effects.

Means designed to hamper satellite operations intentionally are usually referred to as “counterspace capabilities”⁶ or “counterspace measures” (CSMs).⁷ Sometimes, the term “counterspace weapons” is also used to describe all CSMs except cyber intrusion;⁸ however, the word “weapon” is reserved for destructive measures in this report. In some classifications, means of providing situational awareness are also included in the list of CSMs.⁹

In the most general terms, counterspace measures may be divided into (1) kinetic weapons designed to damage or destroy satellite system or its parts physically, (2) non-kinetic weapons which may or may not yield physical damage to targeted object, (3) electronic warfare impacting down- or uplink without directly endangering satellite physically, and (4) various means of

⁶ Swope et al., *Space Threat Assessment* 2024, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-04/240417_Swope_Space_Threat_0.pdf?VersionId=DDeJ0EkYnF5W7POfMJHV-GjKxEVeTx3o0.

⁷ Czajkowski, “Space-Based Systems and Counterspace Warfare”

⁸ Swope et al., *Space Threat Assessment* 2024, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-04/240417_Swope_Space_Threat_0.pdf?VersionId=DDeJ0EkYnF5W7POfMJHV-GjKxEVeTx3o0.

⁹ Weeden and Samson, *Global Counterspace Capabilities* 2024, https://swfound.org/media/207826/swf_global_counterspace_capabilities_2024.pdf.

intrusion through cyberspace. It must also be noted that non-destructive and non-physical measures, which by design are not supposed to bring physical damage or destruction, may ultimately cause such effects due to interference with the satellite's operation.

Various kinetic counterspace measures may affect a space system's ground architecture or its space segment. Ground stations may be attacked by various traditional means of warfare that do not need further description. Space segments may be targeted by what is usually referred to as anti-satellite (ASAT) weapons. They may take the form of ground-based interceptor missiles, called direct-ascent ASAT (DA-ASAT), and space-based, co-orbital (CO-ASAT) systems. They are designed to impact spacecraft directly or with the munition they fire to damage or destroy satellites physically. Attacks of this sort would render a satellite inoperable, turning it into uncontrolled junk, or, highly likely, fragment the targeted craft, contributing to the increased amount of space debris, as described above.

Non-kinetic attacks may involve nuclear explosions, which impact satellites with products such as shockwaves and radiation, or the use of directed energy (DE) devices such as lasers or microwave emitters. If the former is undoubtedly a destructive weapon, the latter need not have to be, which depends on the power of the DE beam. Thus, these weapons may either be destructive, physically impacting satellites in orbit, or they may only render them temporarily inoperative. For example, a laser beam may (1) destroy an observation satellite by an explosion caused by the excessive heat it produces, (2) damage its external structure, rendering it inoperable, (3) permanently blind cameras by destroying their matrices, or (4) only temporarily dazzle the orbiter's optics. So, in the case of DE devices, the distinction between destructive weapons and non-destructive CSMs is somewhat blurred as, in theory, the same systems can be used for both purposes if only their yield can be adjusted. Note that even in the case of a non-destructive attack, a satellite may be rendered uncontrollable, contributing to the contamination of space and increasing the secondary threat the way indicated above.

Electronic warfare impacts the links between space and ground segments of satellite systems. It may be executed in the form of (1) jamming a signal,

making the link unusable, or (2) spoofing it, which means that a false signal is being sent to the receiver. In essence, it is a temporary measure as the jamming/spoofing device may be switched on/off, and the process of jamming/spoofing the signal does not affect receivers in any way. However, if the link used to control a satellite is inoperable for a sufficient time due to jamming/spoofing, its systems may malfunction, which could result in turning it into a space junk with all the well-known consequences.

Cyber-attacks may affect satellite systems in many ways. (1) Data exchanged with the ground station with a downlink or uplink may be corrupted, or (2) intercepted for the adversary's benefit, and (3) the orbiter's control software may be penetrated so that the craft is issued false commands, which can ultimately lead to damage or loss of the satellite with all the secondary effects. Cyber intrusions can target satellites in orbit, ground stations, or end users. The effects of cyber interference on space systems may vary from causing satellites to malfunction, denying users access to the system's services, data falsification, and data theft.

As mentioned in the introduction, this report will not provide detailed information on instances of the use of countermeasures. However, it is worth noting that ASAT weapons have not yet been deployed in militarily significant quantities and have never been used except for testing.¹⁰ On the other hand, non-destructive measures are frequently utilized, particularly dazzling, jamming, or spoofing.

Conclusion

Educational/learning and research satellites may be endangered in various ways, by various methods, and with varying effects. Primary threats to space systems, be they intentional or unintentional, do not necessarily have to concern multiple satellites at the same time. The process of wearing out or unintentional damage/destruction of satellites concerns individual craft and happens occasionally. Naturally, the more satellites that orbit the Earth, the more such occasions occur. Intentional attacks causing permanent effects

¹⁰ Weeden and Samson, *Global Counterspace Capabilities* 2024, https://swfound.org/media/207826/swf_global_counterspace_capabilities_2024.pdf.

may have very limited effects, such as damage to an observation craft's lenses. However, it may also cause serious structural damage, resulting in malfunctioning of the satellite or even its fragmentation. Such destructive attacks may be limited to individual orbiters or may take the form of frequent or even massive warfare in orbit.

As strongly underlined in the argument above, when control over a satellite is lost, whether it has been intentionally destroyed and broken or has just gone defunct out of natural causes, it usually becomes potentially dangerous space junk. The growing probability of collisions with active satellites and space debris is a secondary threat to the safety of space systems. From the point of view of everyday operations and space traffic management, it is the most prominent danger, and it is growing steadily. The more satellites are operating in space now, the more space junk will litter the Earth's orbits in the future. Thus, even without acts of intentional destruction of satellites, the threat to the safe operation of space architecture of every kind is constantly mounting.

It is also worth noting that non-destructive threats are also important from the point of view of the security of education/learning and research process. Every disruption in data flow from or through space architecture or other problems with communication or PNT services might adversely impact the everyday activities of educators and researchers. Additionally, cyber intrusions into space systems may lead to intellectual property theft.

Policy Recommendations

It is imperative for the worldwide scientific community first to understand how threats to space systems impact individual research and education/learning activities, even in fields not related to space science. Secondly, the scientific community must pressure governments to find solutions, seeking alliances with branches of the manufacturing industry and services sectors dependent on satellite systems. Finally, governments and international organizations should prioritize efforts to address the risks associated with increasing contamination of the space environment. International efforts are particularly important, as the danger itself transcends all the earthly boundaries.

Bibliography

- Czajkowski, Marek. "Space-Based Systems and Counterspace Warfare." In *Routledge Handbook of the Future Warfare*, edited by Artur Gruszczak and Sebastian Kaempf Routledge, 2024.
- Kessler, Donald J. and Burton G. Cour-Palais. "Collision Frequency of Artificial Satellites: The Creation of a Debris Belt." *Journal of Geophysical Research* Vol. 86, no. A6 (1978): 2637–2646. <https://archive.org/details/d14ac03de-ada9364f8bb1fd236dfdbbacb1d/page/n9/mode/2up>.
- Swope, Clayton et al. *Space Threat Assessment 2024*. Center for Strategic and International Studies, 2024. https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-04/240417_Swope_Space_Threat_0.pdf?VersionId=DDDe-J0EkYnF5W7POfMJHVGjkkEVeTx3o0.
- Weeden, Brian and Victoria Samson. *Global Counterspace Capabilities 2024*. Secure World Foundation, 2024. https://swfound.org/media/207826/swf_global_counterspace_capabilities_2024.pdf.
- Wright, David, Laura Grego and Lisbeth Gronlund. *The Physics of Space Security*. American Academy of Arts and Sciences, 2005. <https://aerospace.csis.org/wp-content/uploads/2019/06/physics-space-security.pdf>